IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re Application of: Simpson, *et al.*	)	Confirmation No: 8476
	)	Group Art Unit: 2134
Serial No.: 10/002,062	)	
	)	Examiner: Power, William S.
Filed: October 30, 2001	)	
	)	Atty. Docket No.: 10007669-1
For: SECURE PRINTING TO A WEB-BASED	)	
IMAGING PRINT SERVICE	)	

APPEAL BRIEF UNDER 37 C.F.R. § 41.37

Mail Stop: Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Sir:

This Appeal Brief under 37 C.F.R. § 41.37 is submitted in support of the Notice of Appeal filed October 12, 2006, responding to the final Office Action mailed June 12, 2006.

It is not believed that extensions of time or fees are required to consider this Appeal Brief. However, in the event that additional extensions of time are necessary to allow consideration of this paper, such extensions are hereby petitioned under 37 C.F.R. §1.136(a), and any fees required therefor are hereby authorized to be charged to Deposit Account No. 08-2025.

I. Real Party in Interest

The real party in interest is Hewlett-Packard Development Company, LP, a limited partnership established under the laws of the State of Texas and having a principal place of business at 20555 S.H. 249 Houston, TX 77070, U.S.A. (hereinafter "HPDC"). HPDC is a Texas limited partnership and is a wholly-owned affiliate of Hewlett-Packard Company, a Delaware Corporation, headquartered in Palo Alto, CA. The general or managing partner of HPDC is HPQ Holdings, LLC.

II. Related Appeals and Interferences

There are no known related appeals or interferences that will affect or be affected by a decision in this Appeal.

III. Status of Claims

Claims 1-22 stand finally rejected. No claims have been allowed. The final rejections of claims 1-22 are appealed.

IV. Status of Amendments

This application was originally filed on October 30, 2001, with twenty-two (22) claims. In a Response filed July 21, 2005, Applicant amended claims 1, 9, 12, 16, and 18. In a Response filed November 7, 2005, Applicant amended claims 1 and 12. In a Response filed April 19, 2006, Applicant amended claim 12. In a Response filed August 14, 2006, Applicant amended claims 1 and 9 and canceled claims 8 and 10. However, in the Advisory Action of August 23, 2006, the Examiner indicated that the proposed amendments were not entered, since they would allegedly require further consideration and/or search (although matter was being incorporated from dependent claims).

The claims in the attached Claims Appendix (see below) reflect the present state of Applicant's claims.

V. Summary of Claimed Subject Matter

The claimed inventions are summarized below with reference numerals and references to the written description ("specification") and drawings. The subject matter described in the following appears in the original disclosure at least where indicated, and may further appear in other places within the original disclosure.

Embodiments according to independent claim 1 describe a secure method of image production in a web-based imaging environment. The method comprises accessing a destination web service (Figure 1A, 34) and downloading into a browser (Figure 1A, 16), web content (Figure 2, 220) associated with the accessed destination web service (Figure 1A, 34). Applicant's specification, page 16, lines 18-23. The method further comprises downloading into the browser (Figure 1A, 16) a public encryption key (Figure 2, 202) from the accessed destination web service (Figure 1A, 34) and retrieving image data under control of the browser (Figure 1A, 16). Applicant's specification, pages 16-17, lines 5-3. Such a method further comprises encrypting the retrieved image data, wherein the downloaded public encryption key (Figure 2, 202) is utilized as part of the encrypting step. Applicant's specification, pages 16-17, lines 25-3. The method also comprises transmitting the encrypted image data to the accessed destination web service (Figure 1A, 34) and decrypting the encrypted image data by the accessed destination web service (Figure 1A, 34), wherein a private encryption key counterpart (Figure 2, 203) of the public encryption key is utilized as part of the decrypting step. The private encryption key (Figure 2, 203) is accessible exclusively to the accessed destination web service (Figure 1A, 34). Applicant's specification, page 3, lines 1-13; pages 16-17, lines 26-20.

Embodiments according to independent claim 12 describe a computer for providing secure image production in a web-based imaging environment. The computer (Figure 1C, 12) is operable to access a destination web service (Figure 1A, 34) and download web content (Figure 2, 220) from the destination web service (Figure 1A, 34) to a user's browser (Figure 1A, 16). The computer (Figure 1C, 12) is further operable to download a public encryption key (Figure 2, 202) from the destination web service (Figure 1A, 34) to the user's browser (Figure 1A, 16) and encrypt imaging data using the public encryption key (Figure 2, 202) as part of an encryption process. Such a computer (Figure 1C, 12) is also operable to transmit the encrypted imaging data to the destination web service (Figure 1A, 34) and direct the destination web service (Figure 1A, 34) to decrypt the encrypted imaging data using a private encryption key counterpart (Figure 2, 203) of the public encryption key (Figure 2, 202) as part of the decryption process. The private encryption key (Figure 2, 203) is accessible exclusively to the destination web service (Figure 1A, 34). Applicant's specification, page 3, lines 1-13; pages 14-15, lines 23-8; pages 16-17, lines 5-23.

Embodiments according to independent claim 18 describe a system for providing secure image production in a web-based imaging environment. The system comprises a user's browser (Figure 1A, 16) operable to encrypt image data using a first encryption key (Figure 2, 202) as part of an encryption process and to transmit the encrypted image data. The system further comprises a destination web service (Figure 1A, 34) representing a production device (Figure 1B, 154). The web service (Figure 1A, 34) is operable to download the first encryption key (Figure 2, 202) into the user's browser (Figure 1A, 16). The destination web service (Figure 1A, 23) is further operable to receive the transmitted encrypted image data and to decrypt the received encrypted image data using a private encryption key (Figure 2, 203) counterpart of the first encryption key (Figure 2, 202) as part of the decryption process. The system further comprises a data path (Figure 1C, 52) interconnecting the user's browser (Figure 1A, 16) with the destination web service (Figure 1A, 34). Applicant's specification, page 3, lines 1-13; pages 14-15, lines 23-8; pages 16-17, lines 5-23.

VI. Grounds of Rejection to be Reviewed on Appeal

The following grounds of rejections are to be reviewed on appeal:

Claims 1-10, 12-16, and 18-21 have been rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over *Lagarde* (U.S. Patent No. 5,721,908) in view of *Smith* (U.S. Patent No. 6,151,675) in further view of *Vanstone* (U.S. Patent No. 6,134,325).

Claims 11, 17, and 22 have been rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over *Lagarde* in view of *Smith* in further view of *Applied Cryptography* by Bruce Schneier.

VII. <u>Arguments</u>

The Appellant respectfully submits that Applicant's claims 1-7, 9, and 11-22 are patentable under 35 U.S.C. §103. The Appellant respectfully requests that the Board of Patent Appeals overturn the final rejection of those claims at least for the reasons discussed below.

A. Claims 1-7, 9, 12-16, and 18-21

Claims 1-10, 12-16, and 18-21 have been rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over *Lagarde* (U.S. Patent No. 5,721,908) in view of *Smith* (U.S. Patent No. 6,151,675) in further view of *Vanstone* (U.S. Patent No. 6,134,325).

It is well-established at law that, for a proper rejection of a claim under 35 U.S.C. §103 as being obvious based upon a combination of references, the cited combination of references must disclose, teach, or suggest, either implicitly or explicitly, all elements/features/steps of the claim at issue. *See, e.g., In Re Dow Chemical*, 5 U.S.P.Q.2d 1529, 1531 (Fed. Cir. 1988), and *In re Keller*, 208 U.S.P.Q.2d 871, 881 (C.C.P.A. 1981).

1. The *Lagarde* Disclosure

Lagarde discloses that agents on a web server complete tasks in support of a Web browser request. *See* col. 4, lines 36-48. In particular, *Lagarde* describes "providing a web server with a control program agent [which] allows organization of decision support functions to be executed by application processing agent servers located throughout the Internet to gather and supply information not presently available with an existing resources without the need of endless intervention on the part of a requesting user of the WWW; further enabling an ordinary user to take advantage of expertise which is provided by programmable sub-agents developed by those with particular expertise in a given area as well as enabling use of standard routines commonly needed." Col. 5, lines 50-61.

2. The *Smith* Disclosure

Smith describes "encrypt[ing] the document with the public key of a server associated with the recipient of the document, instead of encrypting the document with the public key of the intended recipient." Col. 4, lines 4-7 (Emphasis added). To encrypt the document with the public encryption key of an intended recipient, such as a destination web service, *Smith* describes that the encrypted document would have to be decrypted and then reencrypted by the DDCS server utilizing the public encryption key of the recipient. *See* col. 6, lines 48-60.

3. The *Vanstone* Disclosure

Vanstone describes an RSA (Rivest-Shamir-Adleman) encryption scheme. For example, *Vanstone* discloses:

> Where the data encryption is performed according to an RSA protocol, the recipient 12 will be associated with a pair of keys, one of which is public and the other of which is private. To transmit data from the sender 10 to the recipient 12, the recipients public key is retrieved by the sender. This requires the transmission of a multi-bit key, typically 512 bits but more desirably 1024 bits. This has to be transmitted in a frame format suitable for the protocol.

Col. 2, lines 46-53.

4. Applicant's Claim 1

Applicant's independent claim 1 provides as follows:

> From a user's browser, a secure method of image production in a web-based imaging environment, said method comprising the steps of:
> accessing a destination web service;
> ***downloading into said browser web content associated with said accessed destination web service;***
> ***downloading into said browser a public encryption key from said accessed destination web service;***
> retrieving image data under control of said browser;
> ***encrypting said retrieved image data, wherein said downloaded public encryption key is utilized as part of said encrypting step;***
> transmitting said encrypted image data to said accessed destination web service; and
> decrypting said encrypted image data by said accessed destination web service, wherein a private encryption key counterpart of said public encryption key is utilized as part of said decrypting step, said private encryption key being accessible exclusively to said accessed destination web service.

(Emphasis added).

In the present case, the cited art does not teach or suggest all of the claim limitations, and there is no suggestion or motivation in the cited art to modify the references to include those limitations.

For example, neither *Lagarde* nor *Smith* teaches or suggests "downloading into said browser web content associated with said accessed destination web service," as recited and emphasized above in claim 1, where said image data is encrypted using a download public encryption key from the accessed designation web service and transmitted back to the destination web service.

Also, *Smith* and *Lagarde* are devoid of teachings for downloading web content and public key from a destination web service, where the web content is used to prepare a print job containing image data that is encrypted using the public key of the destination web service.

With regard to *Lagarde*, it teaches that agents on a web server complete tasks in support of a Web browser request. *See* col. 4, lines 36-48. In particular, *Lagarde* teaches "providing a web server with a control program agent [which] allows organization of decision support functions to be executed by application processing agent servers located throughout the Internet to gather and supply information not presently available with an existing resources without the need of endless intervention on the part of a requesting user of the WWW; further enabling an ordinary user to take advantage of expertise which is provided by programmable sub-agents developed by those with particular expertise in a given area as well as enabling use of standard routines commonly needed." Col. 5, lines 50-61.

As such, *Lagarde* fails to suggest retrieving image data under control of a web browser and transmitting the image data to a destination web service, since *Lagarde* teaches that agents at a server perform processing tasks in lieu of a browser application. Additionally, *Smith* and *Vanstone* do not cure the deficiencies of the *Lagarde* reference.

With regard to *Smith*, it teaches "encrypt[ing] the document with the public key of a server associated with the recipient of the document, instead of encrypting the document with the public key of the intended recipient." Col. 4, lines 4-7 (Emphasis added). To encrypt the document with the public encryption key of an intended recipient, such as a destination web service, *Smith* teaches that the encrypted document would have to be decrypted and then reencrypted by the DDCS server utilizing the public encryption key of the recipient. *See* col. 6, lines 48-60.

Therefore, *Smith* is devoid of a teaching for downloading a public encryption key of a destination web service into a browser, since *Smith* discloses that the public key of an intended recipient is not provided to a browser. Moreover, *Smith* teaches that the approach of not providing a public key of an intended recipient to a browser is preferred over an approach where a public key of a destination web service is provided to a browser. In particular, *Smith* clearly states that "**instead of encrypting the document with the public key of the intended recipient**," the document is encrypted "with the public key of a server associated with the recipient of the document." Col. 4, lines 4-7 (Emphasis added). Hence, to modify, the teachings of *Smith* to include the feature of "downloading into said browser a public encryption key from said accessed destination web service" is contrary to the teachings of *Smith*.

As a result, it would not be obvious to combine *Smith* with a reference (*e.g., Vanstone*) that allegedly teaches encrypting a document with a public key of an intended recipient, since *Smith* clearly teaches away from such. Secondarily, *Smith* provides no motivation for doing so. *See ACS Hospital Systems, Inc., v. Montefiore Hospital*, 732 F.2d 1572, 1577; 221 U.S.P.Q. 929, 933 (Fed. Cir. 1984) ("Obviousness cannot be established by combining the teachings of the prior art to produce the claimed invention, absent some teaching or suggestion supporting the combination. Under section 103, teachings of references can be combined *only* if there is some suggestion or incentive to do so."). *See also ALCO Standard Corp. v. Tennessee Valley Authority*, 808 F.2d 1490, 1498, 1 U.S.P.Q.2d 1337, 1343 (Fed. Cir. 1986) ("Moreover, the question is not simply whether the prior art 'teaches' the particular element of the invention, but whether it would 'suggest the desirability, and thus the obviousness, of making the combination.'"); *Lindemann Maschinenfabrik GMBH v. American Hoist and Derrick Co.*, 730 F.2d 1452, 1462, 221 U.S.P.Q. 481 (Fed. Cir. 1984) ("The claimed invention must be considered as a whole, and the question is whether there is something in the prior art as a whole to suggest the desirability, and thus the obviousness, of making the combination.").

For at least these reasons, it would not be obvious to combine the cited portions (or any other portions) of the cited references in order to produce the claimed subject matter. Therefore, a prima facie case establishing an obviousness rejection has not been made by the proposed combination of

Lagarde in view of *Smith* in further view of *Vanstone*. Thus, claim 1 is not obvious in view of the cited references, and the rejection should be withdrawn for at least this reason alone.

5. Applicant's Claims 2-10

Because independent claim 1 is allowable over the cited art of record, dependent claims 2-10 (which depend from independent claim 1) are allowable as a matter of law for at least the reason that the dependent claims contain all the features of independent claim 1. For at least this reason, the rejection of claims 2-10 should be withdrawn.

Additionally and notwithstanding the foregoing reasons for the allowability of claims 2-10, these dependent claims recite further features and/or combinations of features (as is apparent by examination of the claims themselves) that are patentably distinct from the cited art of record. Hence, there are other reasons why these dependent claims are allowable.

With particular regard to claim 8, the cited art fails to teach or suggest at least "choosing desired options represented by said destination web service through said web content," as described in claim 8.

Further with regard to claim 10, the claim recites "creating a print job reflecting said desired options, said print job including said image data." *Smith* and *Lagarde* are devoid of teachings for downloading web content and public key from a destination web service, where the web content is used to prepare a print job containing image data that is encrypted using the public key of the destination web service. Therefore, the cited art fails to teach or suggest at least "creating a print job reflecting said desired options, said print job including said image data," as recited in claim 10.

For example, with regard to *Lagarde*, it teaches that agents on a web server complete tasks in support of a Web browser request. *See* col. 4, lines 36-48. In particular, *Lagarde* teaches "providing a web server with a control program agent [which] allows organization of decision support functions to be executed by application processing agent servers located throughout the Internet to gather and supply information not presently available with an existing resources without the need of endless intervention on the part of a requesting user of the WWW; further enabling an ordinary user to take advantage of expertise which is provided by programmable sub-agents developed by those with particular expertise in a given area as well as enabling use of standard routines commonly needed." Col. 5, lines 50-61.

As such, *Lagarde* fails to suggest claimed features such as retrieving image data under control of a web browser, creating a print job including the image data, and transmitting the image data to a destination web service, since *Lagarde* teaches that agents at a server perform processing tasks in lieu of a browser application. Additionally, *Smith* and *Vanstone* do not cure the deficiencies of the *Lagarde* reference.

For at least these reasons, the rejections should be withdrawn.

6. Applicant's Claim 12

As provided in independent claim 12, Applicant claims:

> A computer for providing secure image production in a web-based imaging environment, said computer operable to:
> access a destination web service;
> ***download web content from said destination web service to a user's browser;***
> ***download a public encryption key from said destination web service to the user's browser;***

> ***encrypt imaging data using said public encryption key as part of encryption process;***
>
> ***transmit said encrypted imaging data to said destination web service;*** and
>
> direct said destination web service to decrypt said encrypted imaging data using a private encryption key counterpart of said public encryption key as part of decryption process, said private encryption key being accessible exclusively to said destination web service.

(Emphasis added).

In the present case, the cited art does not teach or suggest all of the claim limitations, and there is no suggestion or motivation in the cited art to modify the references to include those limitations.

For example, neither *Lagarde* nor *Smith* teaches or suggests "download web content from said destination web service to a user's browser," "download a public encryption key from said destination web service to the user's browser," "encrypt imaging data using said public encryption key as part of encryption process," and "transmit said encrypted imaging data to said destination web service," as recited and emphasized above in claim 12.

With regard to *Lagarde*, it teaches that agents on a web server complete tasks in support of a Web browser request. *See* col. 4, lines 36-48. In particular, *Lagarde* teaches "providing a web server with a control program agent [which] allows organization of decision support functions to be executed by application processing agent servers located throughout the Internet to gather and supply information not presently available with an existing resources without the need of endless intervention on the part of a requesting user of the WWW; further enabling an ordinary user to take advantage of expertise which is provided by programmable sub-agents developed by those with particular expertise in a given area as well as enabling use of standard routines commonly needed." Col. 5, lines 50-61.

Lagarde seemingly fails to suggest encrypting image data and transmitting the image data to destination web service, since *Lagarde* teaches that agents at a server perform processing tasks in lieu of a browser application.

Further, neither *Lagarde* nor *Smith* teaches or suggests "download[ing] a public encryption key from said destination web service to the user's browser," as recited in claim 12. (Emphasis added). For example, *Smith* teaches "encrypt[ing] the document with the public key of a server associated with the recipient of the document, instead of encrypting the document with the public key of the intended recipient." Col. 4, lines 4-7 (Emphasis added). To encrypt the document with the public encryption key of an intended recipient, such as a destination web service, *Smith* teaches that the encrypted document would have to be decrypted and then reencrypted by the DDCS server utilizing the public encryption key of the recipient. *See* col. 6, lines 48-60. Therefore, *Smith* is devoid of a teaching for downloading a public encryption key of a destination web service into a browser, since *Smith* discloses that the public key of an intended recipient is not provided to a browser. Moreover, *Smith* teaches that the approach of not providing a public key of an intended recipient to a browser is preferred over an approach where a public key of a destination web service is provided to a browser. In particular, *Smith* clearly states that "**instead of encrypting the document with the public key of the intended recipient**," a document is encrypted "with the public key of a server associated with the recipient of the document." Col. 4, lines 4-7 (Emphasis added). Thus, to modify, the teachings of *Smith* to include the feature of "download[ing] a public encryption key from said destination web service to the user's browser" is in opposition to the teachings of *Smith*.

As a result, it would <u>not be obvious</u> to combine *Smith* with a reference (*e.g.*, *Vanstone*) that allegedly teaches encrypting a document with a public key of an intended recipient, since *Smith* clearly teaches away from such. Secondarily, *Smith* provides no motivation for doing so. *See ACS Hospital Systems, Inc., v. Montefiore Hospital*, 732 F.2d 1572, 1577; 221 U.S.P.Q. 929, 933 (Fed. Cir. 1984) ("Obviousness cannot be established by combining the teachings of the prior art to produce the claimed invention, absent some teaching or suggestion supporting the combination. Under section 103, teachings of references can be combined *only* if there is some suggestion or incentive to do so."). *See also ALCO Standard Corp. v. Tennessee Valley Authority*, 808 F.2d 1490, 1498, 1 U.S.P.Q.2d 1337, 1343 (Fed. Cir. 1986) ("Moreover, the question is not simply whether the prior art 'teaches' the particular element of the invention, but whether it would 'suggest the desirability, and thus the obviousness, of making the combination.'"); *Lindemann Maschinenfabrik GMBH v. American Hoist and Derrick Co.*, 730 F.2d 1452, 1462, 221 U.S.P.Q. 481 (Fed. Cir. 1984) ("The claimed invention must be considered as a whole, and the question is whether there is something in the prior art as a whole to suggest the desirability, and thus the obviousness, of making the combination.").

Therefore, a prima facie case establishing an obviousness rejection <u>has not</u> been made by the proposed combination of *Lagarde* in view of *Smith* in further view of *Vanstone*. Thus, claim 12 is not obvious in view of the cited references, and the rejection should be withdrawn for at least this reason alone.

7. Applicant's Claims 13-16

Because independent claim 12 is allowable over the cited art of record, dependent claims 13-16 (which depend from independent claim 12) are allowable as a matter of law for at least the reason that the dependent claims contain all the features of independent claim 12. For at least this reason, the rejection of claims 13-16 should be withdrawn.

Additionally and notwithstanding the foregoing reasons for the allowability of claims 13-16, these dependent claims recite further features and/or combinations of features (as is apparent by examination of the claims themselves) that are patentably distinct from the cited art of record. Hence, there are other reasons why these dependent claims are allowable.

With particular regard to claim 16, one of the narrowest claims currently pending, Applicant submits that because of the uniqueness of the claim limitations, claim 16 clearly distinguishes the claimed subject matter over all cited references.

8. Applicant's Claim 18

As provided in independent claim 18, Applicant claims:

> A system for providing secure image production in a web-based imaging environment, said system comprising:
>
> a user's browser operable to encrypt image data using a first encryption key as part of encryption process and to transmit said encrypted image data;
>
> ***a destination web service representing a production device, said web service operable to download said first encryption key into said user's browser, said destination***

> ***web service further operable to receive said transmitted encrypted image data and to decrypt said received encrypted image data using a private encryption key counterpart of said first encryption key as part of decryption process;*** and
>
> a data path interconnecting said user's browser with said destination web service.

(Emphasis added).

In the present case, the cited art does not teach or suggest all of the claim limitations, and there is no suggestion or motivation in the cited art to modify the references to include those limitations. For example, neither *Lagarde* nor *Smith* teaches or suggests "a destination web service representing a production device, said web service operable to download said first encryption key into said user's browser, said destination web service further operable to receive said transmitted encrypted image data and to decrypt said received encrypted image data using a private encryption key counterpart of said first encryption key as part of decryption process," as recited in claim 18.

With regard to *Lagarde*, it teaches that agents on a web server complete tasks in support of a Web browser request. *See* col. 4, lines 36-48. In particular, *Lagarde* teaches "providing a web server with a control program agent [which] allows organization of decision support functions to be executed by application processing agent servers located throughout the Internet to gather and supply information not presently available with an existing resources without the need of endless intervention on the part of a requesting user of the WWW; further enabling an ordinary user to take advantage of expertise which is provided by programmable sub-agents developed by those with particular expertise in a given area as well as enabling use of standard routines commonly needed." Col. 5, lines 50-61.

Lagarde seemingly fails to suggest encrypting image data and transmitting the image data to destination web service, since *Lagarde* teaches that agents at a server perform processing tasks in lieu of a browser application.

With regard to *Smith*, *Smith* teaches "encrypt[ing] the document with the public key of a server associated with the recipient of the document, instead of encrypting the document with the public key of the intended recipient." Col. 4, lines 4-7 (Emphasis added). To encrypt the document with the public encryption key of an intended recipient, such as a destination web service, *Smith* teaches that the encrypted document would have to be decrypted and then reencrypted by the DDCS server utilizing the public encryption key of the recipient. *See* col. 6, lines 48-60. Therefore, *Smith* is devoid of a teaching for downloading a public encryption key of a destination web service into a browser, since *Smith* discloses that the public key of an intended recipient is not provided to a browser. Moreover, *Smith* teaches that the approach of not providing a public key of an intended recipient to a browser is preferred over an approach where a public key of a destination web service is provided to a browser. In particular, *Smith* clearly teaches "encrypt[ing] the document with the public key of a server associated with the recipient of the document, **instead of encrypting the document with the public key of the intended recipient**." Col. 4, lines 4-7 (Emphasis added). Hence, to modify, the teachings of *Smith* to include the feature of "a destination web service representing a production device, said web service operable to download said first encryption key into said user's browser, said destination web service further operable to receive said transmitted encrypted image data and to decrypt said received encrypted image data using a private encryption key counterpart of said first encryption key as part of decryption process" would teach away from *Smith*.

As a result, it <u>would not be obvious</u> to combine *Smith* with a reference (*e.g.*, *Vanstone*) that allegedly teaches encrypting a document with a public key of an intended recipient, since *Smith* clearly teaches away from such. Secondarily, *Smith* provides no motivation for doing so. *See ACS Hospital Systems, Inc., v. Montefiore Hospital*, 732 F.2d 1572, 1577; 221 U.S.P.Q. 929, 933 (Fed. Cir. 1984) ("Obviousness cannot be established by combining the teachings of the prior art to produce the claimed invention, absent some teaching or suggestion supporting the combination. Under section 103, teachings of references can be combined *only* if there is some suggestion or incentive to do so."). *See also ALCO Standard Corp. v. Tennessee Valley Authority*, 808 F.2d 1490, 1498, 1 U.S.P.Q.2d 1337, 1343 (Fed. Cir. 1986) ("Moreover, the question is not simply whether the prior art 'teaches' the particular element of the invention, but whether it would 'suggest the desirability, and thus the obviousness, of making the combination.'"); *Lindemann Maschinenfabrik GMBH v. American Hoist and Derrick Co.*, 730 F.2d 1452, 1462, 221 U.S.P.Q. 481 (Fed. Cir. 1984) ("The claimed invention must be considered as a whole, and the question is whether there is something in the prior art as a whole to suggest the desirability, and thus the obviousness, of making the combination.").

Therefore, a prima facie case establishing an obviousness rejection <u>has not</u> been made by the proposed combination of *Lagarde* in view of *Smith* in further view of *Vanstone*. Thus, claim 18 is not obvious in view of the cited references, and the rejection should be withdrawn for at least this reason alone.

9. Applicant's Claims 19-21

Because independent claim 18 is allowable over the cited art of record, dependent claims 19-21 (which depend from independent claim 18) are allowable as a matter of law for at least the reason that the dependent claims contain all the elements and features of independent claim 18. For at least this reason, the rejection of claims 19-21 should be withdrawn.

B. Claims 11, 17, and 22

Claims 11, 17, and 22 have been rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over *Lagarde* in view of *Smith* in further view of *Applied Cryptography* by Bruce Schneier.

1. The *Lagarde* Disclosure

Lagarde discloses that agents on a web server complete tasks in support of a Web browser request. *See* col. 4, lines 36-48. In particular, *Lagarde* describes "providing a web server with a control program agent [which] allows organization of decision support functions to be executed by application processing agent servers located throughout the Internet to gather and supply information not presently available with an existing resources without the need of endless intervention on the part of a requesting user of the WWW; further enabling an ordinary user to take advantage of expertise which is provided by programmable sub-agents developed by those with particular expertise in a given area as well as enabling use of standard routines commonly needed." Col. 5, lines 50-61.

2. The *Smith* Disclosure

Smith describes "encrypt[ing] the document with the public key of a server associated with the recipient of the document, instead of encrypting the document with the public key of the intended recipient." Col. 4, lines 4-7 (Emphasis added). To encrypt the document with the public encryption key of an intended recipient, such as a destination web service, *Smith* describes that the encrypted document would have to be decrypted and then reencrypted by the DDCS server utilizing the public encryption key of the recipient. *See* col. 6, lines 48-60.

3. The *Applied Cryptography* Disclosure

Applied Cryptography describes various techniques for enciphering and deciphering messages.

4. Applicant's Claims 11, 17, and 22

As noted above, claims 1, 12, and 18 are allowable over the cited art of record. Furthermore, Applicant finds nothing in *Applied Cryptography* to remedy the deficiencies of the cited art regarding claims 1, 12, and 18. Therefore, claims 11, 17, and 22 which depend from respective independent claims 1, 12, and 18 are also allowable.

Additionally and notwithstanding the foregoing reasons for allowability of claims 11, 17, and 22, these claims recite further features and/or combinations of features (as is apparent by examination of the claims themselves) that are patentably distinct from the cited art of record. Accordingly, the rejections to these claims should be withdrawn.

VIII. Conclusion

In summary, it is Applicant's position that Applicant's claims are patentable over the applied cited art references and that the rejection of these claims should be withdrawn. Appellant therefore respectfully requests that the Board of Appeals overturn the Examiner's rejection and allow Applicant's pending claims.

Respectfully submitted,

By: ______________________
Charles W. Griggers
Registration No. 47,283

Claims Appendix under 37 C.F.R. § 41.37(c)(1)(viii)

The following are the claims that are involved in this Appeal.

1. From a user's browser, a secure method of image production in a web-based imaging environment, said method comprising the steps of:

accessing a destination web service;

downloading into said browser web content associated with said accessed destination web service;

downloading into said browser a public encryption key from said accessed destination web service;

retrieving image data under control of said browser;

encrypting said retrieved image data, wherein said downloaded public encryption key is utilized as part of said encrypting step;

transmitting said encrypted image data to said accessed destination web service; and

decrypting said encrypted image data by said accessed destination web service, wherein a private encryption key counterpart of said public encryption key is utilized as part of said decrypting step, said private encryption key being accessible exclusively to said accessed destination web service.

2. The method of claim 1 wherein said retrieved image data is previously referenced to a composition associated with said user's identity.

3. The method of claim 1 wherein said accessed destination web service represents a production device.

4. The method of claim 3 wherein said production device is a printer.

5. The method of claim 1 wherein said retrieving comprises accessing said user's identity from said destination web service via said web content through an imaging extension.

6. The method of claim 1 wherein said retrieving comprises accessing a hard disk local to said web browser.

7. The method of claim 1 wherein said image data is contained in a PDF file.

8. The method of claim 1 further comprising choosing desired options represented by said destination web service through said web content.

9. The method of claim 1 wherein said options include an option to print securely, the option to print securely providing a secure transmission of data to said destination web service.

10. The method of claim 8 further comprising creating a print job reflecting said desired options, said print job including said image data.

11. The method of claim 1 wherein:

said encrypting comprises synthesizing a session key, encrypting said image data using said session key, and encrypting said session key using said public encryption key;

said transmitting further comprises transmitting said encrypted said session key to said destination web service; and

said decrypting comprises decrypting said session key using said private encryption key counterpart of said public encryption key and then using said decrypted said session key to decrypt said encrypted image data.

12. A computer for providing secure image production in a web-based imaging environment, said computer operable to:

access a destination web service;

download web content from said destination web service to a user's browser;

download a public encryption key from said destination web service to the user's browser;

encrypt imaging data using said public encryption key as part of encryption process;

transmit said encrypted imaging data to said destination web service; and

direct said destination web service to decrypt said encrypted imaging data using a private encryption key counterpart of said public encryption key as part of decryption process, said private encryption key being accessible exclusively to said destination web service.

13. The computer of claim 12 wherein said imaging data is previously referenced to a composition associated with a user's identity.

14. The computer of claim 12 wherein said destination web service represents a production device.

15. The computer of claim 14 further operable to direct said destination web service via said web content to select production options for producing said imaging data by said production device.

16. The computer of claim 15 wherein said production options include an option to produce securely, the option to print securely providing a secure transmission of data to said destination web service.

17. The computer of claim 12 further operable to:

synthesize a session key;

encrypt said image data using said session key;

encrypt said session key using said public encryption key;

transmit said encrypted session key to said destination web service; and

direct said destination web service to decrypt said encrypted session key using said private encryption key counterpart of said public encryption key and then to decrypt said encrypted image data using said decrypted session key.

18. A system for providing secure image production in a web-based imaging environment, said system comprising:

a user's browser operable to encrypt image data using a first encryption key as part of encryption process and to transmit said encrypted image data;

a destination web service representing a production device, said web service operable to download said first encryption key into said user's browser, said destination web service further operable to receive said transmitted encrypted image data and to decrypt said received encrypted image data using a private encryption key counterpart of said first encryption key as part of decryption process; and

a data path interconnecting said user's browser with said destination web service.

19. The system of claim 18 wherein said production device is a printer.

20. The system of claim 18 wherein said data path is selected from the group consisting of hard wired data paths and wireless data paths.

21. The system of claim 18 wherein said first encryption key is a public encryption key.

22. The system of claim 21 further comprising a session key, said session key being operable to encrypt said retrieved image data, to be encrypted using said public encryption key, and to be decrypted using said private encryption key counterpart of said public encryption key.

Evidence Appendix under 37 C.F.R. § 41.37(c)(1)(ix)

There is no extrinsic evidence to be considered in this Appeal. Therefore, no evidence is presented in this Appendix.

Related Proceedings Appendix under 37 C.F.R. § 41.37(c)(1)(x)

There are no related proceedings to be considered in this Appeal. Therefore, no such proceedings are identified in this Appendix.